PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PERIODO DE VIGENCIA DEL PLAN
Del 1 de enero al 31 de diciembre de 2023

Personería
Santiago de Cali
Para la Gente

HAROLD ANDRÉS CORTÉS LAVERDE
Personero Distrital
2020 – 2024

Personería Distrital de Santiago de Cali
NIT 805.003.895 - 9
CAM, Torre Alcaldía Piso 13
PBX (2) 6617999
atencionalciudadano@personeriacali.gov.co

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información está basado en los lineamientos presentados en la guía de seguridad y privacidad de información del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC y los estándares ISO 27001:2013, ISO 31000:2018, para establecer los principios e implementar un sistema de gestión de riesgos, cuyo objetivo es minimizar, realizar una gestión y controlar cualquier tipo de riesgo, teniendo en cuenta el origen, la causa y su grado de incidencia, buscando proteger los datos de los ciudadanos y garantizando la seguridad de la información.

Este plan hace parte integral del desarrollo gradual del Plan Estratégico de Tecnologías de Información y las Comunicaciones ***PETI,*** diseñado para el Ente de Control y Vigilancia en línea con la estrategia institucional 2020 - 2024 ***"Personería para la Gente"***.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se encuentra articulado con las políticas contenidas en el Modelo Integrado de Planeación y Gestión MIPG: ***Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción, Gobierno Digital y Seguridad Digital.***

Este documento es propiedad de la Personería Distrital de Santiago de Cali.
Prohibida su reproducción por cualquier medio sin previa autorización.

Contenido

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022 2
1. MARCO NORMATIVO 5
2. ORIENTACIÓN ESTRATÉGICA DE LA PERSONERÍA 6
VISIÓN 6
POLÍTICA DE CALIDAD 7
VALORES 7
3. NIVEL DE GESTIÓN POLÍTICA DE GOBIERNO DIGITAL 2022 8
4. ALINEACIÓN DEL PLAN CON LA ESTRATEGIA INSTITUCIONAL 2020 - 2024 9
5. OBJETIVO GENERAL 10
5.1 Objetivos Específicos. 10
6. ALCANCE 11
7. TÉRMINOS Y DEFINICIONES 11
8. ROLES Y RESPONSABILIDADES 13
9. POLÍTICAS DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN 14
10. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDADY PRIVACIDAD DE LA INFORMACIÓN 15
10.1. SEGURIDAD INFORMÁTICA 15
10.2. NORMA ISO 27001 15
10.3 NORMA ISO 27005:2013. GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN 16
10.4. METODOLOGÍA MAGERIT 21
10.4.1. OBJETIVOS DE LA METODOLOGÍA MAGERIT 21
10.5 ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO FASES DEL PROYECTO 22
10.5.1. DEFINIR EL ALCANCE 22
10.5.2. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN 22

10.5.3. IDENTIFICACIÓN DEL RIESGO 25
10.5.4. IDENTIFICACIÓN DE LAS AMENAZAS 28
10.5.5. IDENTIFICACIÓN DE LA VULNERABILIDAD 29
10.5.6. INDENTIFICACIÓN DE LOS CONTROLES EXISTENTES 30
10.5.7. EVALUACIÓN DE RIESGO 30
10.5.8. VALORACIÓN DE LOS CONTROLES 32
11. METODOLOGÍA 33

1. MARCO NORMATIVO

Constitución Política de Colombia. 1991. Artículo 15.
Ley 44/1993. Por la cual se modifica y adiciona la Ley 23/ 1982 y se modifica la Ley 29/1944.

Ley 527 de 1999. Define y reglamenta el acceso y uso de mensajes de datos, de comercio electrónico y de firmas digitales y se establecen las entidades de certificación.

Ley 594 de 2000. Expide la Ley General de Archivos.

Ley 1266 de 2008. Disposiciones generales del Hábeas Data y regula el manejo de la información contenida en bases de datos personales y la proveniente de terceros países.

Ley 1221 del 2008. Normas para promover y regular el Teletrabajo.

Ley 1273 de 2009. Modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.

Ley 1341 de 2009. Define principios y conceptos sobre la sociedad de la información y la organización TICS

Ley 1474 de 2011. Orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción.

Ley 1581 de 2012. Disposiciones para la protección de datos personales.

Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Ley 1915 de 2018. Modifica la Ley 23 de 1982

Ley 1978 de 2019. Se moderniza el sector de las TIC

Decreto 2609 de 2012. Reglamenta el Título V de la Ley 594/2000, parcialmente los artículos 58 y 59 de la Ley 1437/2011

Decreto 0884 del 2012. Reglamenta parcialmente la Ley 1221/2008.

Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581/2012.

Decreto 886 de 2014. Reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015. Reglamenta parcialmente la Ley 1712/2014

Decreto 1078 de 2015. Expide el Decreto Único Reglamentario del Sector de las TIC.

Decreto 728 de 2017. Adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078/2015, para fortalecer el modelo de Gobierno Digital.

Decreto 1499 de 2017. Modifica Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, relacionado con el Sistema de Gestión establecido en el art. 133 de la Ley 1753/2015.

Decreto 1008 de 2018. Establece lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Dec. 1078/2015, Decreto Único Reglamentario del sector de las TIC.

Decreto 2106 de 2019. Se Dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

Decreto 620 de 2020. Subroga el título 17 de la parte 2 del libro 2 del Dec.1078/2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753/2015, el numeral 3 del artículo 147 de la Ley 1955/2019, y el artículo 9° del Dec. 2106/2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital.

2. ORIENTACIÓN ESTRATÉGICA DE LA PERSONERÍA

MISIÓN

La Personería Distrital de Santiago de Cali como agente del Ministerio Público, salvaguarda el ordenamiento jurídico, representa a la sociedad y vigila la garantía de los derechos humanos, el cumplimiento de los deberes y el desempeño íntegro de quienes ejercen funciones públicas en la Administración Distrital, preservando el proyecto común expresado en la Constitución Política, para producir resultados de valor social, de convivencia y participación, orientados a profundizar la democracia e inclusión con enfoque territorial y diferencial.

VISIÓN

Al 2024, la Personería Distrital de Santiago de Cali será reconocida como un Ente de Control y Vigilancia innovador, confiable, presente en el territorio y cercano a la ***Gente***, portavoz de las poblaciones más vulnerables, oportuno en la acción disciplinaria, con servidores públicos íntegros y diligentes en la atención y servicio a la comunidad, capaz de percibir y procesar los cambios del entorno y actuar conforme a ellos.

POLÍTICA DE CALIDAD

En la Personería Distrital de Santiago de Cali, estamos comprometidos con la satisfacción de la comunidad en el ejercicio diario de las funciones y competencias del Ente de Control y Vigilancia, fundamentado en la vocación de servicio, mediante una atención y respuesta oportuna para el goce de sus derechos, con talento humano competente y capacitado para la mejora continua de la entidad.

VALORES

Los servidores de la Personería Distrital de Santiago de Cali observan, acatan y dan estricta aplicación a los principios establecidos en la Constitución Política, las Leyes y los Reglamentos; en especial los contenidos en el Código Disciplinario.

Las conductas dentro y fuera de la entidad de los servidores de la Personería Distrital de Santiago de Cali, se orientan por los valores y principios de acción del Código de Integridad del Servicio Público Colombiano adoptado mediante la Resolución 262 del 30 de agosto de 2018 y fijado en la Ley 2016 del 27 de febrero de 2020, y cumplen un carácter esencial para el cabal cumplimiento de la misión, visión y objetivos institucionales.

HONESTIDAD **R**ESPETO **C**OMPROMISO **D**ILIGENCIA **J**USTICIA

PROBIDAD **S**OLIDARIDAD

Ver Resolución No. 122 del 1 de junio de 2020

3. NIVEL DE GESTIÓN POLÍTICA DE GOBIERNO DIGITAL 2022

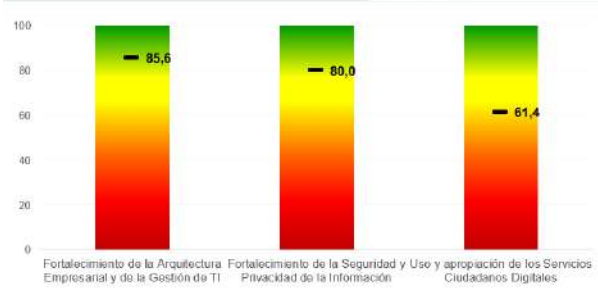
Nivel de Gestión vigencia 2021

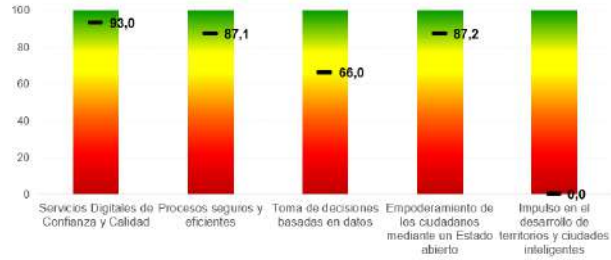
Puntaje	Nivel	Color
0 - 20	1	
21 - 40	2	
41 - 60	3	
61- 80	4	
81- 100	5	

En una escala de 1 a 100, el nivel de gestión al 31 de diciembre de 2022 se ubica en el nivel 4 (Color amarillo) lo que confirma que se encuentra documentado, opera y está actualizado frente a las normas y requisitos legales aplicables a la entidad.

Las acciones de mejora para el año 2023 corresponden a la programación durante la vigencia para el seguimiento y evaluación de los componentes contenidos en el Plan de Tratamiento de Riesgos y Privacidad de la Información.

Nivel de avance en la implementación de la Política de Gobierno Digital	Escala de 0 - 100
Bajo	Menor a 20
Medio bajo	Igual o mayor a 20 y menor a 40
Medio	Igual o mayor a 40 y menor a 60
Medio alto	Igual o mayor a 60 y menor a 80
Alto	Igual o mayor a 80 y menor o igual a 100





4. ALINEACIÓN DEL PLAN CON LA ESTRATEGIA INSTITUCIONAL 2020 - 2024

La alineación del Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información con el Plan Estratégico Institucional PEI 2020 – 2024 ***"Personería para la Gente"*** adoptado mediante la Resolución No. 122 de junio 1 de 2020, está contenida en el Artículo 4 a través del Objetivo Estratégico 2.1.

Objetivo Estratégico.

"Potenciar la gestión interna de la Personería Distrital de Santiago de Cali de cara a la figura distrital de la ciudad, a través de procesos ágiles, simples y flexibles, para lograr mejor desempeño institucional con efectos diferenciadores en la prestación de los servicios y un talento humano íntegro, diligente y comprometido".

LINEA ESTRATÉGICA:	Institucional
Indicador de Resultado:	Índice de Desempeño Institucional
Programa:	Fortalecimiento Institucional
Meta Producto:	100% PETI Desarrollado y Evaluado

Ver Resolución No. 122 del 1 de junio de 2020

5. OBJETIVO GENERAL

Mitigar los riesgos informáticos en la Personería Distrital de Cali mediante la aplicación de la norma ISO 27005-2013 con el fin de proteger los activos de información de la entidad, preservando la confidencialidad, integridad y disponibilidad.

5.1 Objetivos Específicos.

a. Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo.

b. Categorizar y valorar los activos e información.

c. Establecer los controles y políticas de seguridad de la información que garantice la confidencialidad, integridad y disponibilidad de la información.

d. Proyectar el mapa de riesgo informático de la Personería Distrital de Santiago de Cali.

e. Definir a través de una adecuada administración del riesgo; una base confiable para la toma de decisiones y la planificación institucional.

6. ALCANCE

Este documento tiene como premisa mejorar el análisis, la evaluación y el control de los riesgos de seguridad, generadas por las actividades diarias y el uso de la información institucional en la Personería Distrital de Santiago de Cali. En el proceso de minimizar y prevenir los riesgos se definen roles y responsabilidades para todos los funcionarios y contratistas, aprobados en el Comité de Gestión y Desempeño.

7. TÉRMINOS Y DEFINICIONES

Activo: Es un recurso que tiene un valor específico para la entidad y debe ser protegido.

Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.

Análisis de brecha: Es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

Análisis de riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.

Acciones asociadas: Son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo.

Administración de riesgos: Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: Situación externa que no controla la entidad y que puede afectar su operación.

Causa: Medios, circunstancias y/o agentes que generan riesgos.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Evento: Acción que pudo haber causado daño, pero fue controlado.

Evento de seguridad: Situación previamente desconocida que puede ser relevante para la seguridad.

Gestión de Riesgo Informático: Actividades empleadas para mitigar los riesgos informáticos

Información: Conjunto de datos que tiene un significado.

Incidente de Seguridad Informática: Daño que puede comprometer las operaciones de la Entidad.

ISO: Organización Internacional de Normalización, es una organización para la creación de estándares internacionales.

Impacto: Daño que provoca la materialización de una amenaza.

Mapa de riesgos: Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Materialización del riesgo: Ocurrencia del riesgo identificado.

Probabilidad: Posibilidad de que una amenaza se materialice.

Protección de Datos: Ley que reconoce y protege el derecho que tienen las personas a conocer, actualizar y rectificar la información que hayan recogido sobre ellas (Base de Datos, Archivos susceptibles de tiramiento por entidades de naturaleza Pública o Privada).

PHVA: Planear, Hacer, Verificar, Actuar.

Riesgo: Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

SGSI: Sistema de Gestión de Seguridad de la Información.

Seguridad de la información: Es un conjunto de medidas preventivas y reactivas de las organizaciones. Sistema tecnológico que permite resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos.

Seguridad Informática: Es la encargada de la seguridad en el medio informático; también llamada ciberseguridad, la cual se ocupa de la implementación técnica y de la operación para la protección de la información.

Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien conozca alguna técnica o método de ataque.

8. ROLES Y RESPONSABILIDADES

Es primordial tener claridad sobre los objetivos institucionales y estratégicos de la entidad, tener una visión sistémica de la gestión, de manera que se analicen las oportunidades o amenazas relevantes, que puedan generar riesgos y afecten el cumplimiento de los objetivos misionales de la entidad, formulados en el Plan Estratégico PEI 2020-2024.

8.1. Proceso Gestión Tecnológica y de la Información:

La construcción del Plan de Tratamiento de Riesgos es responsabilidad del Proceso Gestión Tecnológica y de la Información. La administración de los riesgos de seguridad y privacidad depende de la participación de todo el equipo de funcionarios y contratistas de la Personería Distrital de Santiago de Cali.

8.2. Oficina Asesora de Planeación:

Se encarga de evaluar y aprobar las directrices para la administración del riesgo y ejecución de controles, con el objetivo de minimizar los riesgos que afecten las gestiones de los procesos y la entidad.

8.3. Líderes de los Procesos:

Se encargan de identificar los riesgos y establecer acciones para mitigarlos, analizando las causas, proponiendo acciones y presentando evidencias para el plan de mejoramiento de los procesos.

9. POLÍTICAS DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

- Implementar la Política de Seguridad y Privacidad de la información.
- Identificar aspectos organizativos de la seguridad de la información en los procesos.
- Seguridad de la Información enfocada a los recursos humanos.
- Revisión de los Controles de acceso.
- Eventos de riesgo en los procesos.
- Gestión de incidentes de Seguridad de la Información.

Para minimizar los riesgos es importante sean asignados recursos humanos, tecnológicos, operativos y de presupuesto, que permitan de una manera continua desarrollar esquemas de trabajo y actividades para mejorar las políticas de seguridad y privacidad existentes.

10. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

10.1. SEGURIDAD INFORMÁTICA

La Seguridad Informática y la Seguridad de la Información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integral y disponibilidad de la información.

Ilustración 1: Pilares de la Seguridad Informática.

10.2. NORMA ISO 27001

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de Gestión de Seguridad de la Información de una empresa o entidad. Investiga cómo salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

MODELO PHVA DEL SGSI

Un SGSI establece una serie de procesos y lineamientos que se deben seguir mediante la estandarización de la norma ISO 27001 para asegurar los activos de información de una organización, como base de datos, oficios, actas, información sensible, entre otros. El objetivo es mantener siempre la triada de la información (Confidencialidad, Integridad y Disponibilidad de la Información).

Ilustración 2: Ciclo PHVA de SGSI

10.3 NORMA ISO 27005:2013. GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

ISO 27005 es un estándar internacional que se ocupa de la gestión de riesgo de seguridad de la información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa o entidad (Personería Distrital de Cali), apoyando los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

Contiene diferentes procedimientos y directrices que permiten establecer los riesgos que enfrenta una organización y la posibilidad de mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación del riesgo, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riegos.

El no contar con una buena gestión de la seguridad de la información para la Personería Distrital de Santiago de Cali puede traer consecuencias negativas como pérdida, fuga o robo de información, alteración de documentos, negación de servicios, entre otros.

“Las secciones contenidas en la norma ISO 27005 son:

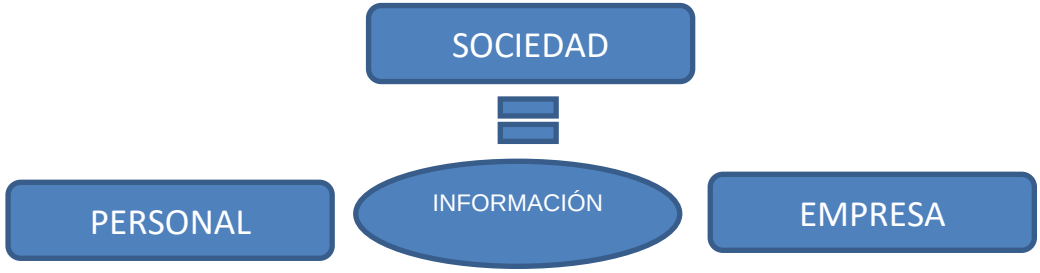
- Prefacio.
- Introducción.
- Referencias normativas.
- Términos y definiciones.
- Estructura.
- Fondo.

- Descripción general del proceso de ISRM.
- Establecimiento de contexto.
- Evaluación de riesgos de seguridad de la información.
- Seguridad de la información (Aceptación del riesgo).
- Seguridad de la información (Comunicación de riesgos).
- Seguridad de la información (Monitoreo y revisión de riesgos).
- Anexo A: Definición del alcance del proceso.
- Anexo B: Valoración de los Activos y evaluación de impacto.
- Anexo C: Ejemplos de amenazas típicas.
- Anexo D: Vulnerabilidades y métodos de evaluación de vulnerabilidad.
- Anexo E: enfoques ISRA.

Es necesario un enfoque sistemático para la gestión de riesgo en la seguridad de la información para identificar las necesidades de la Personería Distrital de Cali, con respecto a los requisitos de seguridad de la información y para crear un sistema de gestión de la seguridad de la información (SGSI) eficaz. Este enfoque debe ser adecuado para el entorno de la Personería Distrital de Santiago de Cali y debería cumplir los lineamientos de toda la gestión de riesgo en la entidad.

La gestión de riesgo en la seguridad de la información debería contribuir a:

- Identificación de los riesgos.
- La valoración de los riesgos en término de sus consecuencias para el negocio (Personería Distrital de Santiago de Cali) y la probabilidad de su ocurrencia.
- La comunicación y el entendimiento de la probabilidad y las consecuencias de los riesgos.
- El establecimiento del orden por prioridad para el tratamiento de los riesgos.
- La priorización de las acciones para reducir la ocurrencia de los riesgos.
- La participación de los interesados cuando se toman las decisiones sobre la gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo.
- La eficiencia del monitoreo del tratamiento de riesgo.
- El monitoreo y revisión con regularidad del riesgo y los procesos de la gestión de riesgos.
- La captura de información para mejorar el enfoque de la gestión de riesgos.
- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos.



- FOTOS EN REDES SOCIALES
- UBICACIÓN (VIAJES, LUGAR HABITUAL DE VACACIONES)
- INFORMACIÓN FINANCIERA

- DOCUMENTACIÓN (PLANTILLAS, PROCEDIMIENTOS)
- INFORMACIÓN DEL NEGOCIO
- CÓDIGO FUENTE
- INFORMACIÓN DE CLIENTES
- INFORMACIÓN DE FACTURACIÓN

La sociedad como tal debe compartir información. Hay dos tipos de información que se puede compartir:

La información personal y la información empresarial.

La información que manejamos, ya sea de tipo personal o empresarial tiene asociado un riesgo.

La palabra riesgo se asocia a problemas que se pueden omitir y que pueden afectar negativamente en nuestra vida.

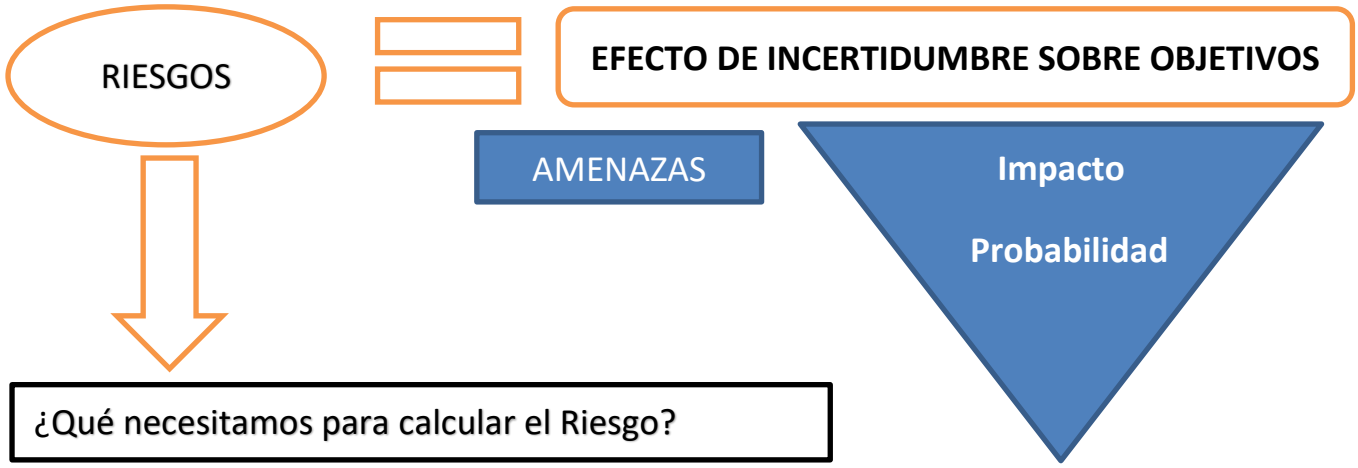
El riesgo es un efecto de incertidumbre sobre un objetivo. Ejemplo: un ciclista que disputa una etapa de 200 kilómetros. El objetivo para él es terminar la etapa – la incertidumbre es que el transcurso de la competencia sufra una caída o por motivo ambiental, suspenda la etapa y no pueda terminar.

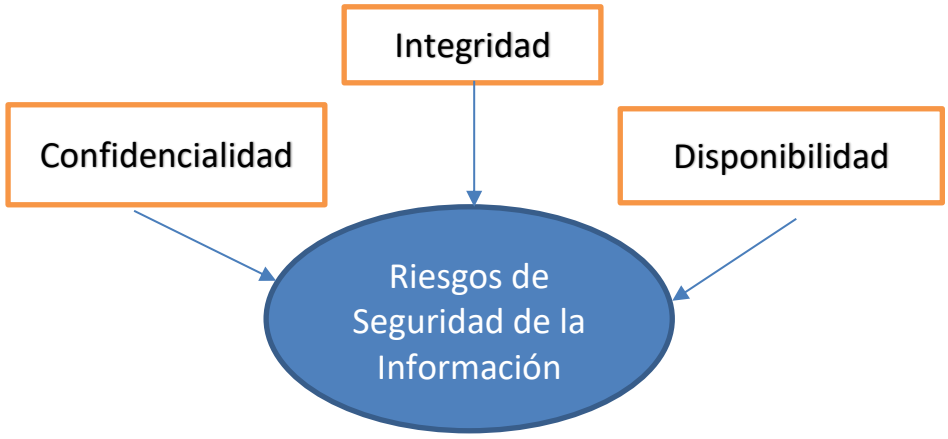
Entonces, el objetivo es terminar la etapa; todo lo que pueda ocurrir en la carrera que afecte negativamente y no permita terminarla, son riesgos.

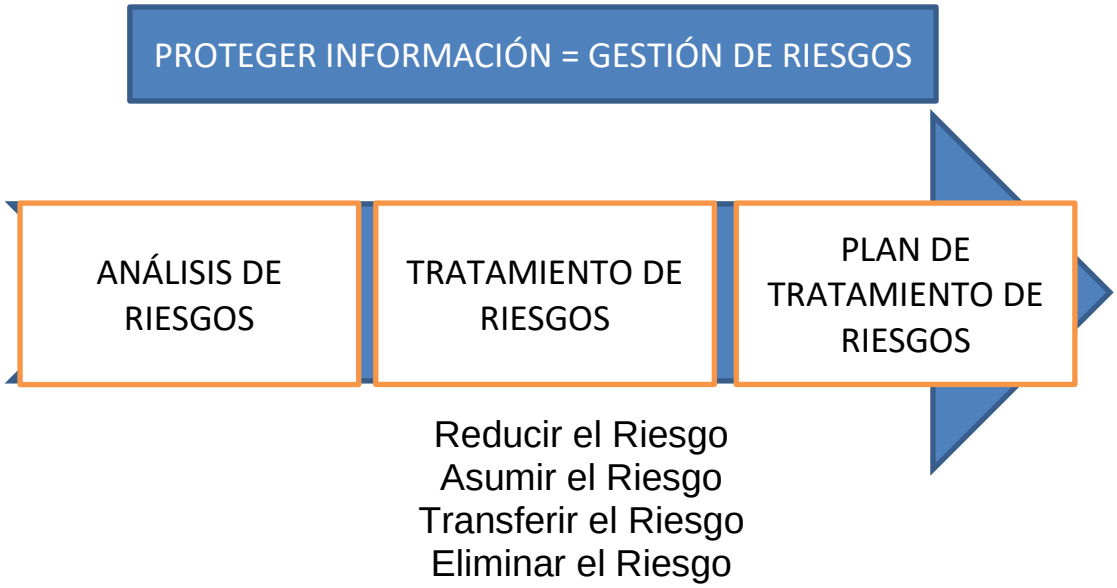
¿Cómo puedo determinar este riesgo? Lo puedo determinar con una fórmula que se compone de dos parámetros: el impacto y la probabilidad.

Cuando hablamos de impacto, nos referimos al conjunto de consecuencias que origina un riesgo sobre mi objetivo. Ejemplo: un funcionario de la Personería Distrital de Cali tiene como objetivo enviar una información por correo electrónico. Existe la incertidumbre de que la información se recepcione de forma íntegra. Dichos riesgos pueden provocar que la información no llegue a su destino. La amenaza refiere a que alguna persona no autorizada, pueda acceder a la información, se interrumpa, modifique o divulgue el mensaje y de esa forma se vulnere la privacidad entre el emisor y el receptor del mensaje.

El riesgo lo puedo determinar calculando la probabilidad de que la amenaza se localice y su respectivo impacto sobre la continua operación de la organización.







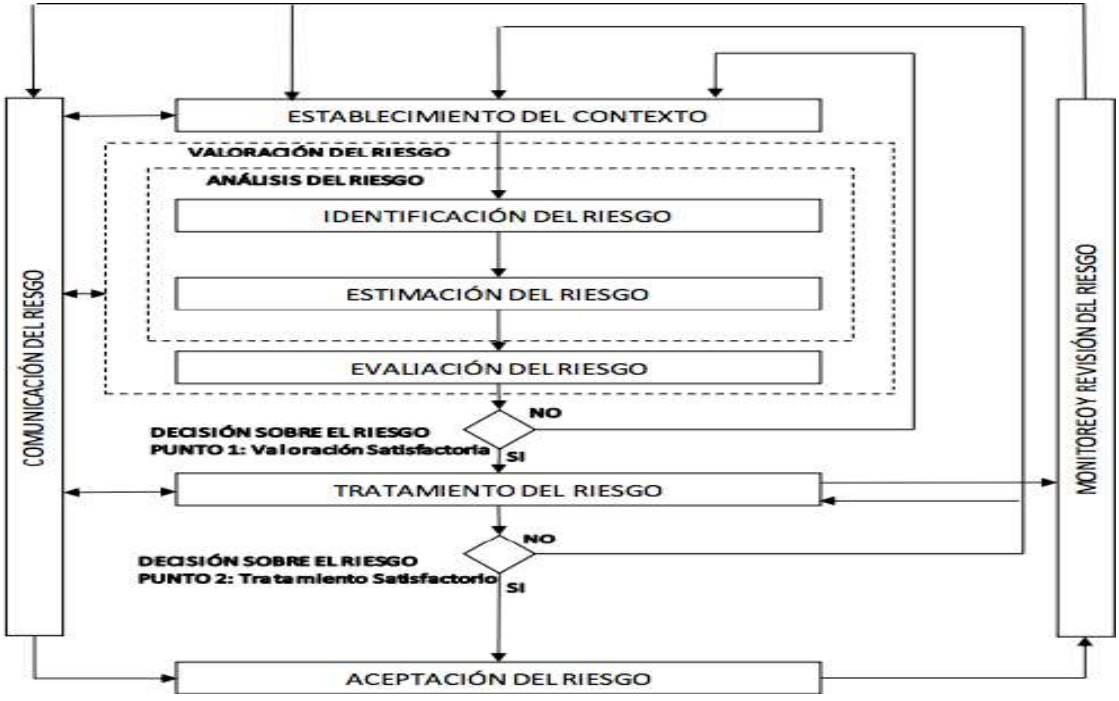


Ilustración 3. Proceso para la administración de riesgos de seguridad y privacidad de la información
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Para la evaluación de riesgos de seguridad y privacidad de la información se tomará como insumo la matriz de Activos de Información, sobre la cual se implementará el presente Plan sobre los Activos de Información que tengan un nivel alto de clasificación al evaluar los criterios de confidencialidad, integridad y disponibilidad, según los siguientes criterios.

10.4. METODOLOGÍA MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), se basa en analizar el impacto que puede tener una organización al ser vulnerada, buscando identificar las amenazas que puede llegar a afectar el funcionamiento de la compañía.

Esta metodología, guía paso a paso cómo llevar a cabo el análisis de riesgos y está dividida en tres partes:

La primera parte hace referencia al método, donde se describe la estructura que debe tener el modelo de gestión de riesgos de acuerdo con la norma ISO 27001.

La segunda parte es el inventario de activo de información que puede utilizar la empresa para enfocar el análisis de riesgos, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

La tercera parte son las técnicas que contienen ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo-beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

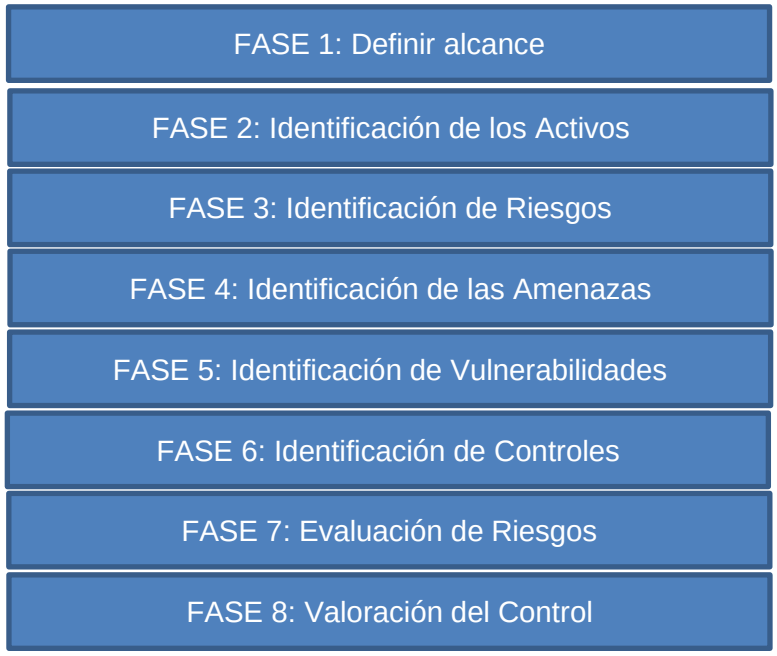
10.4.1. OBJETIVOS DE LA METODOLOGÍA MAGERIT

- Concientizar a los funcionarios y responsables de la información, los riesgos que enfrentan y cómo mitigarlos.

- Establecer el tratamiento de los riesgos para evitar que se materialicen.

- Proyectar a las organizaciones para la auditoría y certificación de la Norma ISO 27001.

10.5 ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO FASES DEL PROYECTO



10.5.1. DEFINIR EL ALCANCE

En esta fase se establecen los objetivos, la justificación del procedimiento que se va a realizar, los funcionarios implicados y el contexto de seguridad informática con el que cuenta la Personería Distrital de Santiago de Cali.

10.5.2. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

El principal activo de una organización es la información, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en discos duros externos, memorias USB o en forma digital, en los equipos de cómputo o en la nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización).

Se diseñó un formato de inventario de activos de información que contiene los siguientes campos:

Nombre del líder del proceso / Nombre del funcionario, Norma, Función del Proceso/ Función que realiza el funcionario.

TIPO DOCUMENTAL:

Nombre del activo de información/ Nombre correspondiente al activo de información como Base de Datos, Actas, Informes, Sistemas de Información, entre otros.

Descripción del Activo de información:

TIPOLOGÍA:

Software / el activo de información se encuentra en forma digital.
Hardware/ el activo de información se encuentra en físico.
Servicios/ el activo de información se emplea como servicio a terceros. (Documentos físicos).

TIPO DE SOPORTE (Medio de conservación y/o Soporte):

Análogo/ Copia adicional del documento en forma física.
Digital / Copia de seguridad en otro equipo, en correo electrónico o en la nube.
Electrónico/ Copia de seguridad en equipo. Electrónico como Disco Duro Externo USB.

Presentación de la información (formato o extensión); en qué aplicación se realiza el activo de información.
Ej.: Formato Portátil de Documento, Word, Excel, entre otros.

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN:

Nivel del Criterio

Tabla 1: Evaluación de la confidencialidad

Confidencialidad / se evalúa con los siguientes valores:

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que pueden ser conocida y utilizada sin autorización por cualquier persona, sea empleado o no de la Personería Distrital de Santiago de Cali.	Público
1	Información que puede ser conocida y utilizada por todos los empleados de la Personería Distrital de Santiago de Cali y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la	Reservada - Uso Interno

	Personería Distrital de Santiago de Cali, el Sector Público Nacional o terceros.	
2	Información que solo puede ser conocida y utilizada por un grupo de empleados que la necesiten para realizar su trabajo y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Personería Distrital de Santiago de Cali.	Reservada-Confidencial
3	Información que solo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Personería Distrital de Santiago de Cali, y cuya divulgación o uso no autorizado podría ocasionar perdidas graves o hacia terceros.	Reservada-Secreta

Tabla 2: Evaluación de Integridad

Integridad / se evalúa con los siguientes valores:

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente o afecta la operación de la Personería Distrital de Santiago de Cali.
1	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas leves para la Personería Distrital de Santiago de Cali.
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Personería Distrital de Santiago de Cali o hacia terceros.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la Personería Distrital de Santiago de Cali o hacia terceros.

Tabla 3: Evaluación de la Disponibilidad

Disponibilidad / se evalúa con los siguientes valores:

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operación de la Personería Distrital de Santiago de Cali.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la Personería Distrital de Santiago de Cali.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Personería Distrital de Santiago de Cali o hacia terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la Personería Distrital de Santiago de Cali o hacia terceros.

Estado de la información / si la información es variable o constante.

Localización del documento o del activo de información / Numero de Equipo o Archivador.

Publicada en (Link Web Page).

Área /Dependencia.

Observaciones.

10.5.3. IDENTIFICACIÓN DEL RIESGO

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Pérdida, Robo o Fuga de Información	- Fallas en el proceso de copia de respaldo o de restauración de la información o pérdida de la misma. - Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de TI. - No contar con acuerdos de confidencialidad con los empleados y terceros. - Falta de autorización para la extracción de información generadas por requerimientos. - Ingresos a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad. - Habilitación de los puertos USB en modo de lectura y escritura para medio de almacenamiento. - Ataques cibernéticos internos o	- Afectación parcial o total de la continuidad de las operaciones de los servicios. - Incumplimiento normativo. - Vulneración de los sistemas de seguridad operando actualmente. - Mala imagen. - Multas, sanciones y pérdidas económicas. - Generación de consultas, funcionalidades o reportes con información sensible de los clientes. - Pérdida o fuga de

	externos. - Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - Prestar los equipos informáticos a personal no autorizados. - No cerrar sesión cuando se desplaza del puesto. - Acceso no autorizado a las oficinas. - Conectar dispositivos externos a los equipos. - Falta de implementación de la política de escritorio limpio.	información.
Correos electrónico de extraña procedencia	- Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - No generar una cultura de Seguridad de la Información. - Falta de filtro en el servidor de correo. - Programas de DLP (Data Lost prevention). - Falta de instalación de Endpoint (Programa de Seguridad punto final) en las estaciones de trabajo.	- Cifrado de la información. - Captura de las pulsaciones del teclado. - Monitoreo de las actividades en el equipo. - Ataques remotos mediante un troyano. - Robo de contraseña. - Equipo usado como zombie para Bonnet (usado para atacar otros DDos). - Robo de documentos y/o archivos.

		- Sistema con mal funcionamiento.
Daño en los equipos tecnológicos	- Manejo inadecuado de los equipos. - Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas. - Falta de equipos de potenciación. - Fallas por defecto de fábrica. - Derrame de líquido. - Falta de ambiente adecuado para los equipos. - Falta de educación a los usuarios en el manejo de los equipos de cómputo.	- Pérdida de información. - Pérdida de los equipos informáticos. - Indisponibilidad del servicio. - Traumatismo en los procesos.
Dumpsterdivind (buceo en la basura)	- Desconocimiento del riesgo. - Falta de capacitación y conciencia.	- Creación de perfil de ataque. - Captura de información privilegiada.
Pérdida de conectividad.	- Daño extremo de ISP (Internet Service Provider). - Ataque DDos (denegación de servicios distribuidos o denegación de servicios)	- Pérdida del Servicio Temporal. - Que un Servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provoca perdida de la conectividad con la red por el consumo de ancho de banda.
Ataques informáticos	- Estimulo o reto personal. - Rebelión. - Ánimo de lucro. - Espionaje.	- Daños en los equipos tecnológicos. - Incidente en la confiabilidad, integridad y disponibilidad de la

		información. - Denegación de servicio. - Secuestro de la información. - Divulgación ilegal de la información. - Suplantación de identidad. - Destrucción de la información. - Soborno de la información.

El objetivo de la identificación de riesgos es conocer los incidentes o eventos que puede causar pérdidas o alteraciones en el funcionamiento de la Personería Distrital de Santiago de Cali y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

La identificación de los riesgos se realiza con observación directa, ingeniería social y con el análisis a los equipos de seguridad perimetral. Por confidencialidad de la Personería Distrital de Santiago de Cali, se presenta la identificación de riesgo General:

Tabla 4: identificación de Riesgos Informáticos

10.5.4. IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño a los activos de la organización. Las amenazas pueden ser de origen humano o ambiental.

Tabla 5: Identificación de amenazas

AMENAZA	TIPO
Polvo, corrosión	Eventos naturales
Inundación	Eventos naturales
Incendios	Eventos naturales

Fenómenos sísmicos	Eventos naturales
Fenómenos Térmicos	Eventos naturales y daños físicos
Pérdida en el suministro de energía	Daño físico
Espionaje remoto	Acciones no autorizadas
Ingeniería social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Acceso forzado al sistema	Acciones no autorizadas
Manipulación del Hardware	Acciones no autorizadas
Fallas del Equipo	Fallas técnicas
Saturación del Sistema de Información	Fallas técnicas

10.5.5. IDENTIFICACIÓN DE LA VULNERABILIDAD

Las vulnerabilidades son las fallas o debilidades en un sistema que pueden ser explotadas por quien conozca métodos de ataque.
Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso, es necesario conocer la lista de amenazas y el inventario de activos de información.

Tabla 6: Identificación de la Vulnerabilidades

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las oficinas.	No existe un control para el acceso de las personas no autorizadas a las oficinas.
Falta de dispositivos de seguridad biométrica para acceder a las oficinas de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de aplicación de la política de escritorio limpio.	La política de escritorio limpio es implementada para que los funcionarios no dejen expuestos: Documentos, equipos electrónicos u objetos de valor sobre los escritorios.
Falta de máquina trituradora de papel.	La máquina trituradora de papel evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.
Falta de capacitación de los funcionarios en tema de seguridad informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y cómo mitigarlos.
Faltas de equipos electrónicos para copias de respaldos.	El no contar con un HDD externo impide a los funcionarios realizar copias de respaldo.
Falta de equipos institucionales.	El no contar con suficientes equipos

	institucionales conlleva a los funcionarios a traer equipos personales que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente, promueve el compartir de cuentas de usuarios y claves que pueden afectar al prestar dichos equipos.
Equipo clon.	Los equipos clones no cuentan con software legal, lo cual puede infectar le red o traer problemas legales.

10.5.6. INDENTIFICACIÓN DE LOS CONTROLES EXISTENTES

La identificación de los controles existentes permite realizar la evaluación de riesgos. Los controles garantizan que al momento de la materialización de un riesgo se reduzca o mitiguen los riesgos informáticos y la organización funcione correctamente, pero se debe tener en cuenta que nunca van a estar 100% seguros.

Dada la importancia de los controles con los que cuenta la Personería Distrital de Santiago de Cali, no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

10.5.7. EVALUACIÓN DE RIESGO

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genere el riesgo en los activos de información, dado por la matríz de calificación, evaluación y respuesta a los riesgos.

La metodología que se emplea para la evaluación de riesgo es MARGERIT.

Tabla 7: Probabilidad de Riesgo

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos cinco años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos cinco años.
3	Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 8: Impacto del Riesgo

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCION**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 9: Matriz de Calificación, Evaluación y Respuesta a los Riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de Riesgo Baja: Asumir el Riesgo.
M: Zona de Riesgo Moderada: Asumir el Riesgo, Reducir el Riesgo.
A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o Transferir.
E: Zona de Riesgo Extrema: Reducir el Riesgo, Evitar, Compartir o Transferir.

10.5.8. VALORACIÓN DE LOS CONTROLES

La valoración de controles evalúa los controles existentes en la organización y la efectividad para mitigar la exposición al riesgo.

Se emplea una tabla para la valoración del control donde se establecen dos parámetros con cinco criterios dependiendo del puntaje y, si el control se ejecuta con la probabilidad, con el impacto o con ambos, se genera un desplazamiento del valor del riesgo.

Tabla 10: Valoración de los Controles

VALORACIÓN DE CONTROL		
PARÁMETROS	**CRITERIOS**	**PUNTAJE**
HERRAMIENTAS PARA EJERCER EL CONTROL	Posee una herramienta para ejercer el control.	15
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta.	15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.	30
SEGUIMIENTO AL CONTROL	Están definidos los responsables de la ejecución del control y del seguimiento.	15
	La frecuencia de ejecución del control y seguimiento es adecuada.	25
TOTAL		**100**

Tabla 11: Evaluación de los Controles

CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO, DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	PROBABILIDAD	IMPACTO
ENTRE 0 -50	0	0
ENTRE 51-75	1	1
ENTRE 76-100	2	2

11. METODOLOGÍA

Gestión de Riesgos				
Actividad	**Tarea**	**Responsable**	**Fecha Inicio**	**Fecha Final**
Sensibilización institucional sobre Política de Seguridad de la Información.	Realizar la divulgación de las reglas de comportamiento adecuadas para el uso de los sistemas y la información de la entidad.	Proceso Gestión Tecnológica y de la Información	01/11/2022	28/02/2023
Identificación de riesgos de seguridad y privacidad de la información.	Evaluación de los activos y amenazas.	Proceso Gestión Tecnológica y de la Información- Líder Política Gobierno Digital	01/11/2023	28/02/2023
Inventario de Activos.	Analizar los activos vinculados a la información.	Proceso Gestión Tecnológica y de la Información- Líder Política Gobierno Digital	01/03/2023	28/04/2023
Elaborar procedimientos gestión de Riesgos de seguridad de la Información.	Realizar la revisión de los actuales procedimientos con el objeto de identificar las necesidades de documentación y/o actualización.	Proceso Gestión Tecnológica y de la Información- Líder Política Gobierno Digital	01/05/2023	30/06/2023

Gestión de Riesgos				
Actividad	**Tarea**	**Responsable**	**Fecha Inicio**	**Fecha Final**
Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información	Definir una metodología de gestión del riesgo enfocada a procesos que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información.	Proceso Gestión Tecnológica y de la Información- Líder Política Gobierno Digital	03/07/2023	17/07/2023
Identificación de Riesgos	Conocer los eventos potenciales, estén o no bajo el control de la entidad, que ponen en riesgo el logro de su misión.	Oficina Asesora de Planeación	18/07/2023	31/08/2023
Análisis de Riesgos	Establecer la probabilidad de ocurrencia de los riesgos y sus consecuencias, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de riesgo.	Oficina Asesora de Planeación	01/09/2023	29/09/2023
Valoración del riesgo.	Comparar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos.	Oficina Asesora de Planeación	02/10/2023	16/10/2023
Evaluación de Controles.	Determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo.	Oficina de Control Interno en conjunto con los procesos.	17/10/2023	31/10/2023

Gestión de Riesgos				
Actividad	**Tarea**	**Responsable**	**Fecha Inicio**	**Fecha Final**
Socialización y Comunicación Políticas de Riesgos.	Dar a conocer a funcionarios, contratistas y terceros de la Entidad, las políticas de tratamiento de riesgos de Seguridad y Privacidad de la Información mediante el uso de las herramientas de comunicaciones disponibles en la Entidad.	Proceso Gestión Tecnológica y de la Información- Líder Política Gobierno Digital	01/11/2023	13/11/2023
Monitoreo y Revisión al Tratamiento de los Riegos.	El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se lleven a cabo y evalúen la eficacia en su implementación.	Oficina de Control Interno.	14/11/2023	Permanente

Gestión Tecnológica y de la Información

Addy Johanna Salcedo Londoño, Líder del Proceso yLíder Política de Gobierno y Seguridad Digital

Diego Cardona Campo, Jefe Oficina Asesora de Planeación (E) - Revisión Técnica

Personería
Santiago de Cali
Para la Gente

Ley de Transparencia y Acceso a la Información
www.personeriacali.gov.co